Ecube

La blockchain

Puidoux, 4 mai 2018

Charles Weinmann
Président honoraire Weinmann-Energies SA

Weinmann-Energies SA
Ingénieurs-conseils EPFL-SIA-USIC

Contenu

- Définition
- Explication
- Comment ça marche
- Exemples (Bitcoin, centrales villageoises, Etherum, …)
- Conclusions

2

Définition

Technologie de stockage et de transmission d'information qui est sécurisée, transparente et qui fonctionne sans organe central de contrôle, le fichier central est réparti sur un réseau d'ordinateurs.

Les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiées et groupées à intervalles de temps réguliers en blocs, l'ensemble étant sécurisé par cryptographie (langage secret), et forment ainsi une chaîne.

3

Explication

Dans une comptabilité, on a un registre de comptes. Ce registre comprend plusieurs pages, chaque page est un bloc.

Les blocs achevés ne peuvent plus être modifiés.

- Internet réduit les distances (protocole TCP/IP)
- La blockchain se passe d'intermédiaires et établit la confiance, sécurise les blocs (idéalisme communautaire).

4

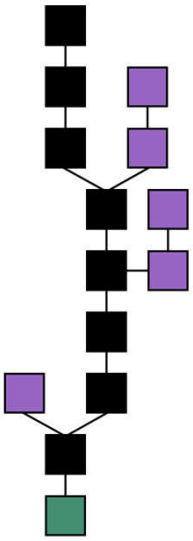
Explication

C’est un registre qui contient des données, des informations, des transactions regroupées en blocs

D’où le nom : chaîne de blocs.

5

Chaîne de blocs



6

Caractéristiques

- Il existe des blockchains publiques, ouvertes à tous
- … et des blockchains privées, limitées à un cercle d'acteurs

7

Explication 1

Une blockchain contient l'historique de tous les échanges effectués entre les utilisateurs depuis sa création. Elle est partagée par tous ces utilisateurs, sans intermédiaires, ce qui permet à chacun de vérifier la validité de la chaîne.

C'est un grand livre comptable que tout le monde peut lire, mais impossible à effacer ou à modifier, à moins d'un consensus des utilisateurs.

Il n'est pas entre les seules mains d'une seule instance, banque ou Etat.

8

Explication 2

Chaque bloc est validé par des nœuds du réseau, à l'aide d'algorithmes

Il y a plusieurs sortes d'algorithmes (protocoles informatiques).

Ils valident les transactions et les contrats passés à l'aide d'un algorithme, ce qui permet à tous les utilisateurs de se mettre d'accord sur l'état du registre en un temps t.

Dans les bitcoins, les nœuds du réseau sont appelés des «mineurs» qui sont les utilisateurs du réseau.

9

Explication 3

Une plateforme rassemble toutes les données (de production et de consommation dans le cas de l'énergie).

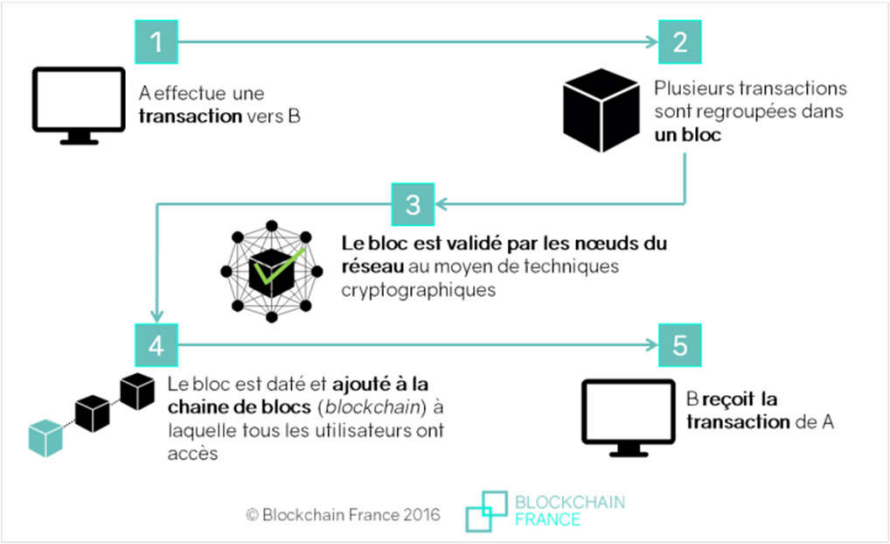
Analogie avec un grand livre de comptes où chacun a une page

Analogie avec une symphonie où les partitions musicales sont réparties entre tous les musiciens.

Personne n'a la partition du chef d'orchestre (toutes les données)

10

Transaction



11

Exemples

Il y a 3 catégories d'utilisation:

- Transferts d'actifs
- Blockchain en tant que registre
- Les smart contracts.

Exemples:

- Bitcoin
- Centrales villageoises
- Etherum
- Droits d'auteurs (YouTube)

12

Bitcoin

La Blockchain est apparue en 2008 avec la monnaie numérique bitcoin. La validation du bloc se fait selon la technique «proof-of-work, preuve de travail)» qui consiste en la résolution d'un algorithme et qui requiert de la puissance de calcul

=> consomme de l'électricité.

13

Bitcoin

- On assiste actuellement à une nouvelle ruée vers l'or... mais virtuelle celle-ci. Pour générer des nouveaux Bitcoin, on fait travailler des ordinateurs (mineurs) inlassablement. Celui qui répond le premier à une question gagne le droit de créer un nouveau bloc dans la Blockchain... et gagne automatiquement de nouveaux bitcoins.

14

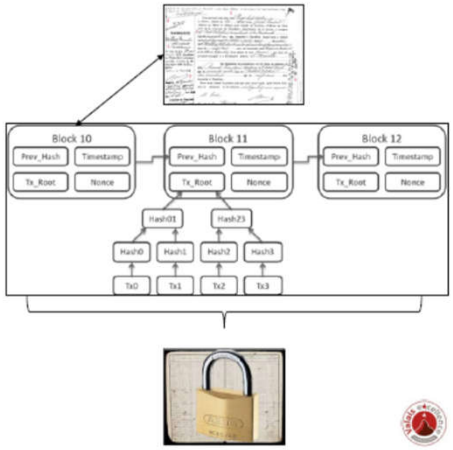
Sécurisation de la blockchain

1) Un bloc ne peut être modifié ou supprimé

2) Chaque bloc est constitué des éléments suivants :

- Timestamp
- Une somme de contrôle (« hash »), utilisée comme identifiant
- La somme de contrôle du bloc précédent

3) Pour écrire un bloc, le réseau doit être d'accord (plus de tiers de confiance)



HES-SO Valais-Wallis
Page 12

15

Les mineurs pour les bitcoins

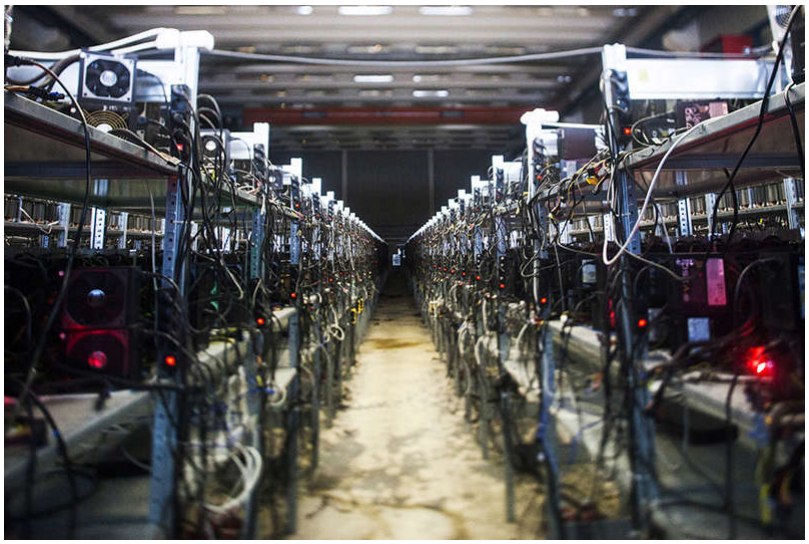
Que font les ordinateurs qui minent ? Ils essaient de résoudre un problème mathématique.
Plus précisément, ils essaient de trouver "le nombre qui, hashé, donne un nombre commençant par une longue série de zéros".

Les mineurs doivent retrouver quel nombre, une fois hashé, commence par une série de zéros

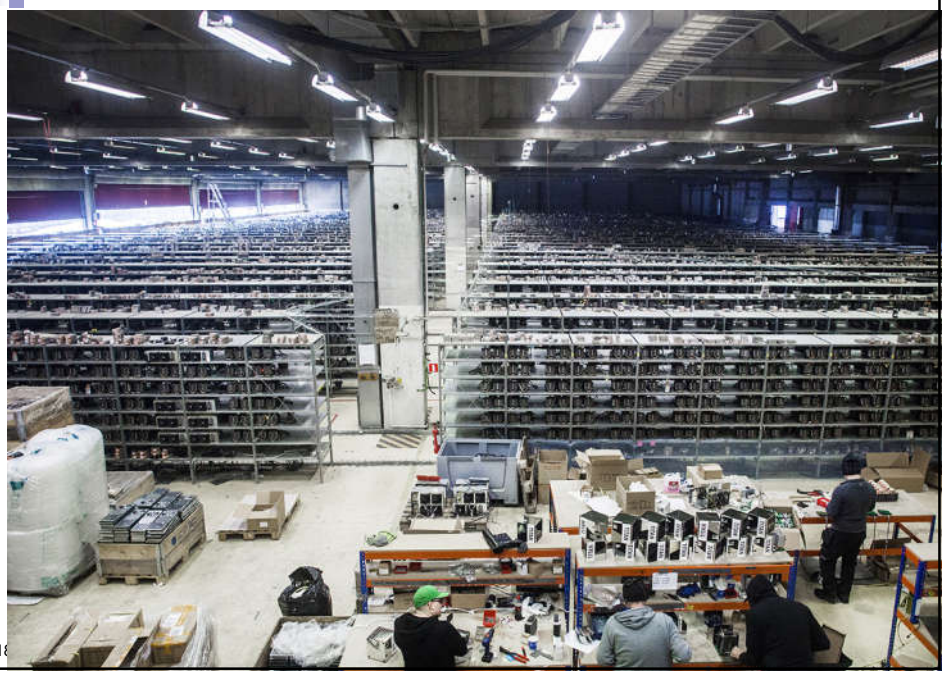
Hash

? → 0000000000XXXXXXXXXXXXXXXXXXXXXX

16



17



18

Constatations

- La blockchain n'est pas un produit fini, mais un processus évolutif.
- Nouveaux algorithmes: preuves de travail, preuve de participation, preuve d'existence, preuve d'enjeu,…
- La blockchain est stockée sur des serveurs
- Bitcoin: n'importe qui peut se raccorder au réseau par un programme, «bitcoin core»
- La réponse aux questions devient de plus en plus difficile

19

Constatations

- Le processus prend une dizaine de minutes pour bitcoin, 15 s pour Etherium
- Grands défis avec menaces et opportunités
- AXPO avec WKW, crée une plateforme ELBOX
- Citibank souhaite créer sa propre cryptomonnaie Citicoin
- La blockchain change les modèles d'affaire

20

Blockchain pour l'énergie

- L'énergie possède de nombreuses facettes, de l'extraction à la consommation, susceptibles de rendre l'utilisation des blockchains intéressante.
- La période est favorable : la multiplication des auto-producteurs pose d'important problèmes aux réseaux de distributions traditionnels, conçus historiquement de façon univoque.
- La solution prônée pour y répondre est celle de la multiplication des réseaux locaux intelligents, les smart-grids. Des projets en développement représentent aujourd'hui une partie du potentiel de la technologie blockchain dans cette perspective.

21

La blockchain et l'électricité

Les proconsumers génèrent de l'énergie qu'ils autoconsomment. Le solde est livré sur le grid a travers un compteur.

Les flux d'énergies sont automatiquement encodés dans un registre de la blockchain

Des algorithmes lient les vendeurs et les consommateurs en temps réel en fonction de préférences et encodent des smart contrats dans la blockchain

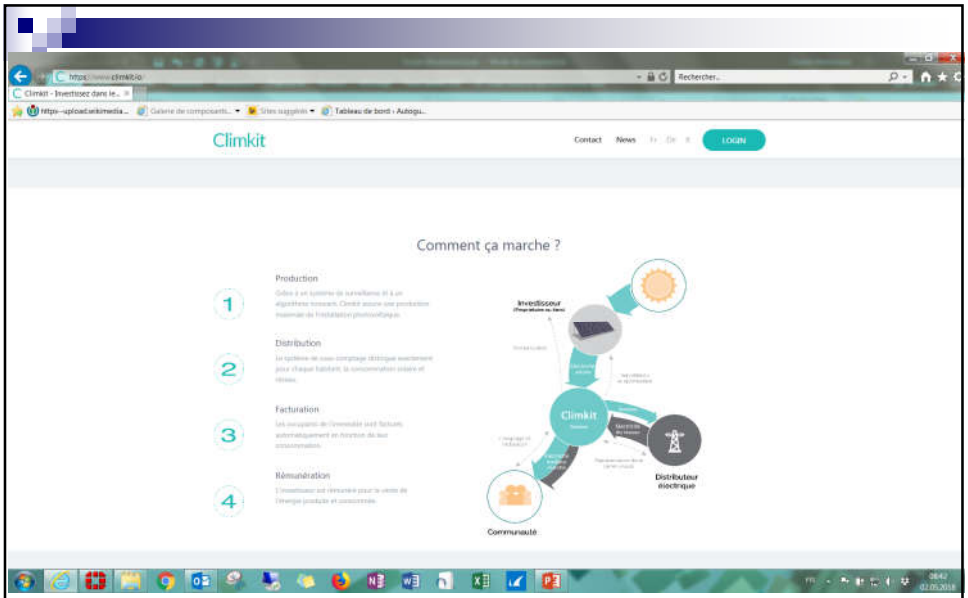
Le smart contrat sont exécutés lorsque les consommations est délivrée, transfère le payement dans une monnaie scripturale de l'acheteur au vendeur

Les autres partenaires de la blockchain vérifient automatiquement la transaction

Lux Reasearch,inc

HES-SO Valais-Wallis
Page 11

22



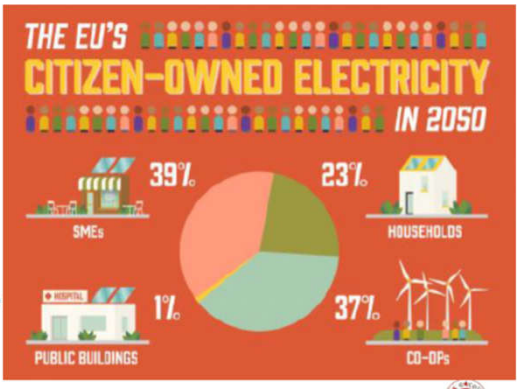
23

RESCOOP.EU

Hes·so VALAIS WALLIS

Fédération européenne des coopératives d'énergie renouvelable

- un réseau de plus de 1'200 coopératives
- Le soutien direct aux projets coopératifs (gestion de projet, financement, contacts, etc)
- La communication en faveur de ce modèle auprès des législateurs européens.



24

Centrale villageoise

Extrait du Prof. Stéphane Genoud au club RAVEL

Comment arriver à demain?

Hes·so VALAIS WALLIS

Actuellement, l'énergie des centrales villageoise est vendue au distributeur, mais demain elle pourra être vendue entre paires, grâce à l'introduction des développements de la technologie **blockchain** dans le concept des **centrales villageoises.**

25

Développements

- Il faut bien passer par une plateforme
- On recrée de nouveaux services ailleurs
- Nouvelle infrastructure des échanges
- Evolution se fait pas à pas

26

Quelques définitions

- Smart contracts
- ICO (Initial coin offering), token = jetons

27

Les smart contrats constituent l'un des types d'usage les plus prometteurs de la blockchain. Concrètement, il s'agit de **programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable et inscrites dans la blockchain**. Ils fonctionnent comme toute instruction conditionnelle de type « if – then » (si telle condition est vérifiée, alors telle conséquence s'exécute).

28

Pour illustrer un usage possible des smart contracts, prenons **l'exemple des assurances voyage** : constatant que 60 % des passagers assurés contre le retard de leur vol ne revendiquaient jamais leur argent, une équipe a créé lors d'un hackathon à Londres en 2015 un système d'assurance automatisé basé sur des smart contracts. Avec ce service, **les passagers sont automatiquement indemnisés lorsque leur vol est en retard, sans avoir besoin de remplir un quelconque formulaire**, et donc sans que l'entreprise ne doive traiter les demandes. Pour se déclencher, le smart contract se connecte à une base de données définie au préalable comme fiable, en l'occurrence dans ce cas une base de données de l'aéroport.

29

Une ICO (Initial Coin Offering) est une **méthode de levée de fonds (crowd founding), fonctionnant via l'émission d'actifs numériques (tokens = jetons) échangeables contre des cryptomonnaies durant la phase de démarrage d'un projet.**

Dans une premier temps, les tokens sont émis par l'organisation à l'origine de l'ICO, et peuvent être acquis par quiconque lors de l'ICO en échange de cryptomonnaie (le plus souvent, de l'ether ou du bitcoin).
Dans un second temps, ces tokens

- sont vendables et achetables sur des plateformes d'échange, à un taux dépendant de l'offre et de la demande. Ils sont donc **très liquides**.
- ont vocation à être **utilisables dans le projet** financé par l'ICO en question. Leur valeur est donc censée dépendre du service fourni in fine par l'entreprise à l'origine de l'ICO.

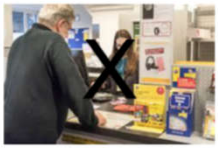
30

Etherium , une application de la blockchain

Hes·so VALAIS WALLIS

L' Ehterium est plateforme décentralisée basée sur la blockchain: l'application permet de passer des smartcontracts automatiquement (presque) sans risque.

C' est la possibilité d'écrire un **contrat** sous la forme de code, qui **automatise des transactions**



Comprendre Ethereum

Ethereum est considérée comme la blockchain la plus prometteuse en dehors de Bitcoin. Ses créateurs en parlent comme du « premier véritable ordinateur global», qui permet de construire sur sa plateforme des **applications décentralisées**.

« *Ethereum vise à bâtir un Web où les intermédiaires entre les clients et les services qu'ils recherchent n'existent plus. Si je veux, par exemple, conclure un contrat numérique avec vous, pourquoi est-ce que j'aurais besoin d'un avocat pour cela? Mettons-nous d'accord sur les modalités de ce contrat. Dans l'infrastructure d'Ethereum, celui-ci n'est pas modifiable ou falsifiable puisque sa sécurité est garantie par un protocole cryptographique. On s'économise des frais d'avocat tout en gagnant en sécurité. Cette idée peut s'appliquer à d'autres services comme les réseaux sociaux, les sites de financement participatif, eBay, Airbnb, UBER, Climkit, Elblox, ….*»

Conclusion 1

Bouleverse les transferts d'argent qui peuvent être faits en quelques minutes.

Nouveau modèle de confiance.

C'est un service comme UBER, mais sans UBER

Il faut une plateforme de change

Nombreuses questions juridiques, économiques, politiques, de gouvernance, écologiques, à résoudre.

33

Conclusion 2

- La blockchain est en pleine évolution
- Grand développement des coopératives d'autoconsommation.
- Conférences annoncées:
- CEES, Neyruz, autoconsommation, 17 mai
- Energy forum VS le 12 juin. Stéphane Genoud de la HES SO-VS est un leader dans ce domaine

34

Merci de votre attention

35